552, 744

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Oktober 2004 (21.10.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/090695 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2004/001807

(22) Internationales Anmeldedatum:
24. Februar 2004 (24.02.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 16 951.2 12. April 2003 (12.04.2003) DE

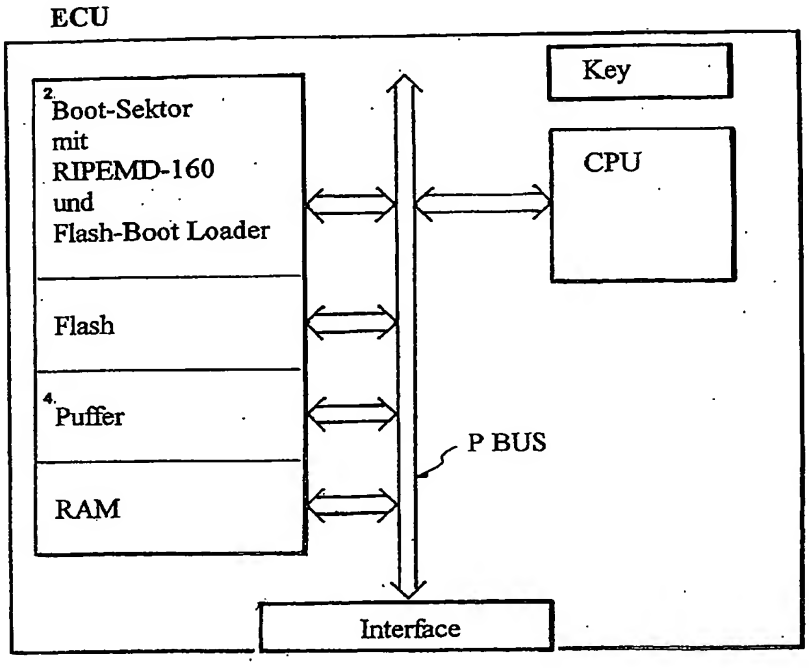
(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DAIMLERCHRYSLER AG** [DE/DE]; Epplestrasse 225, 70567 Stuttgart (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **KOBER, Heiko** [DE/DE]; Hauprstrasse 7, 75365 Calw (DE). **SCHNEIDER, Jutta** [DE/DE]; Kressbacher Strasse 12, 72072 Tübingen (DE). **WIESER, Eva** [DE/DE]; Mörikestrasse 69, 70199 Stuttgart (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR CHECKING THE DATA INTEGRITY OF SOFTWARE IN CONTROL APPLIANCES

(54) Bezeichnung: VERFAHREN ZUR ÜBERPRÜFUNG DER DATENINTEGRITÄT VON SOFTWARE IN STEUERGERÄTEN



2. BOOT SECTOR WITH RIPEMD-160 AND FLASH BOOT LOADER
4. BUFFER

(57) Abstract: In order to check the data integrity of software for transmission errors and authenticity during a downloading process, the flashed data must be repeatedly checked. The access to program data stored in the flash memory, or the access time, is time-intensive. A long access time with complex calculations, such as an authenticity check, leads to long and unbearable delays, especially for control appliances in motor vehicles which generally have low calculation powers for financial reasons. According to the invention, the checking of program data for transmission errors and authenticity can be efficiently designed, if the calculation methods for checking for transmission errors and authenticity are carried out as long as the flash program is located in a buffer memory with a rapid access time. Time-intensive access to the flash memory is thus avoided. If, until now, the flash memory had to be accessed each time the flash program was checked, according to the inventive method, the flash memory need only be accessed once, in order to intermediately store the flash program in a buffer memory with rapid access time, for all required checks.

(57) Zusammenfassung: Bei einer Überprüfung der Datenintegrität von Software bei einem Downloadprozess auf Übertragungsfehler und Authentizität müssen die geflashten Daten mehrmals überprüft werden. Der Zugriff bzw. die Zugriffszeit auf Programmdaten, die im Flachspeicher abgelegt sind, ist zeitintensiv. Besonders bei Steuergeräten im Kraftfahrzeug, die aus Kostengründen in der Regel über geringe

[Fortsetzung auf der nächsten Seite]

WO 2004/090695 A1

(74) **Anwälte: ESCHBACH, Arnold** usw.; DaimlerChrysler AG, Intellectual Property Managment, IPM - C106, 70546 Stuttgart (DE).

(81) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Rechenleistungen verfügen, führt eine lange Zugriffszeit bei aufwendigen Berechnungen, wie einer Authentizitätsprüfung, zu langen und unerträglichen Verzögerungen. Erfindungsgemäss kann die Überprüfung von Programmdaten auf Übertragungsfehler und Authentizität effizient gestaltet werden, wenn die Berechnungsverfahren zur Überprüfung auf Übertragungsfehler und für die Überprüfung auf Authentizität durchgeführt werden, solange sich die Flachware in einem Pufferspeicher mit schneller Zugriffszeit befindet. Zeitintensive Zugriffe auf den Flachspeicher werden dadurch vermieden. Musste bisher für jede Überprüfung der Flachware auf den Flachspeicher zugegriffen werden, so muss nach dem erfindungsgemässen Verfahren lediglich einmal auf den Flachspeicher zugegriffen werden, um die Flachware für alle notwendigen Überprüfungen in einen Pufferspeicher mit schneller Zugriffszeit zwischenzuspeichern.

Verfahren zur Überprüfung der Datenintegrität von Software in Steuergeräten

Die Erfindung betrifft ein Verfahren zum Aktualisieren und Laden von zumindest einem Anwenderprogramm, einer sogenannten Flashware, das in einem Programmspeicher eines Mikroprozessorsystems gespeichert werden soll. Der Downloadprozess erfolgt hierbei über eine Systemschnittstelle. Der Programmspeicher ist in einen elektrisch lösch- und programmierbaren Speicher, einen sogenannten Flash, und in einen flüchtigen Schreiblesespeicher, einem sogenannten Random Excess Memory, unterteilt. Bevor die herunterzuladende Flashware in dem Flashspeicher abgelegt wird, erfolgt eine Überprüfung der heruntergeladenen Programmdaten auf Integrität und Authentizität.

Ein Verfahren zum Aktualisieren und Laden von Anwenderprogrammen in einem Programmspeicher eines Mikroprozessorsystems ist aus der deutschen Patentschrift DE 195 06 957 C2 bekannt. Hier wird über eine Systemschnittstelle eine Flashware in den Flashspeicher eines Mikroprozessorsystems eingelesen. Die Flashware wird hierbei zunächst in einem statischen Schreiblesespeicher, einem sogenannten Static Random Excess Memory (SRAM), zwischengespeichert und mittels eines zyklischen Blocksicherungsverfahrens auf Übertragungsfehler überprüft. Eine Überprüfung auf Authentizität des heruntergeladenen Flashwareprogramms findet hierbei nicht statt.

Andererseits ist aus der deutschen Offenlegungsschrift DE 100 08 974 A1 ein Signaturverfahren für die Authentizitätsprüfung einer Flashware für ein Steuergerät in einem Kraftfahrzeug bekannt. Bei diesem Verfahren wird die Flashware mit einer sogenannten elektronischen Unterschrift versehen. Zur Erstellung der elektronischen Unterschrift wird von der Flashware mittels der an sich bekannten Hash-Funktion ein sogenannter Hash-Code generiert. Dieser Hash-Code wird mittels eines Public-Key-Verfahrens verschlüsselt. Als Public-Key-Verfahren wird vorzugsweise das RSA-Verfahren, benannt nach den Erfindern Rivest, Shamir und Adleman, eingesetzt. Der verschlüsselte Hash-Code wird dem zu übertragenden Anwendungsprogramm angehängt. Im Steuergerät wird der verschlüsselte Hash-Code mit dem öffentlichen Schlüssel entschlüsselt und mit dem im Steuergerät berechneten Hash-Code über die Flashware verglichen. Stimmen beide Hash-Codes überein, ist die übertragene Flashware authentisch. Eine Überprüfung auf Übertragungsfehler ist dem Signaturverfahren nicht zu entnehmen.

Ausgehend von dem vorbeschriebenen Stand der Technik ist es Aufgabe dieser Erfindung, ein Verfahren zur Überprüfung der Datenintegrität von Software in Steuergeräten vorzuschlagen, bei dem die übertragenen Daten in möglichst effizienter Weise auf Übertragungsfehler und Authentizität überprüft werden können.

Die erfindungsgemäße Lösung gelingt mit einem Verfahren mit den Merkmalen des unabhängigen Anspruchs. Vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Unteransprüchen und in der Beschreibung der Ausführungsbeispiele enthalten.

Bei einer Überprüfung der Datenintegrität von Software bei einem Downloadprozess auf Übertragungsfehler und Authentizität müssen die geflashten Daten mehrmals über-

prüft werden. Der Zugriff bzw. die Zugriffszeit auf Programmdaten, die im Flashspeicher abgelegt sind, ist zeitintensiv. Besonders bei Steuergeräten im Kraftfahrzeug, die aus Kostengründen in der Regel über geringe Rechenleistungen verfügen, führt eine lange Zugriffszeit bei aufwendigen Berechnungen, wie einer Authentizitätsprüfung, zu langen und unerträglichen Verzögerungen. Erfindungsgemäß kann die Überprüfung von Programmdaten auf Übertragungsfehler und Authentizität effizient gestaltet werden, wenn die Berechnungsverfahren zur Überprüfung auf Übertragungsfehler und für die Überprüfung auf Authentizität durchgeführt werden, solange sich die Flashware in einem Pufferspeicher mit schneller Zugriffszeit befindet. Zeitintensive Zugriffe auf den Flashspeicher werden dadurch vermieden. Musste bisher für jede Überprüfung der Flashware auf den Flashspeicher zugegriffen werden, so muss nach dem erfindungsgemäßen Verfahren lediglich einmal auf den Flashspeicher zugegriffen werden, um die Flashware für alle notwendigen Überprüfungen in einen Pufferspeicher mit schneller Zugriffszeit zwischenzuspeichern.

Der mit der Erfindung hauptsächlich erzielte Vorteil liegt in der zeitlich effizienten Berechnung von mehreren Prüfsummen und ggf. einer zusätzlichen Signaturprüfung durch Reduzierung der Zugriffe auf den Flashspeicher. Dies ermöglicht kürzere Flashzeiten für den Downloadprozess und damit etliche Einsparungen an Produktionszeit.

Für die Authentizitätsprüfung werden vorteilhafterweise an und für sich selbst bekannte Verfahren eingesetzt. Etablierte Standards sind z. B. die RSA-Signatur von Flashware oder die Verwendung eines sogenannten Message Authentication Code. Beide vorgenannten Authentizitätsprüfungen können mit Vorteil im Zusammenhang mit der Erfindung eingesetzt werden.

In einer alternativen Ausführung des erfindungsgemäßen Verfahrens erfolgt vor der Authentizitätsprüfung eine Abfrage und eine Auswahl der für die Authentizitätsprüfung anzuwendenden Sicherheitsklasse. Damit ist die Erfindung sowohl für Flashware mit einer niederen Sicherheitsklasse als auch für Flashware mit einer hohen Sicherheitsklasse einsetzbar.

Im Folgenden wird die Erfindung anhand der Ausführungsbeispiele gemäß der Figuren 1 bis 3 näher erläutert.

Es zeigen:

Fig. 1 ein Blockdiagramm eines beispielhaften Steuergerätes mit einem Mikroprozessor und einer logisch funktionellen Aufteilung des Speicherbereichs.

Fig. 2 eine exemplarische Aufteilung eines Speichers in logische Blöcke, wobei jeder logische Block aus mehreren Segmenten bestehen kann. Die programmierten Daten (Flashware) werden in den Segmenten abgelegt. Die Lücken zwischen den Segmenten werden mit sogenanntem illegal opcode oder illegal data aufgefüllt.

Fig. 3 ein Ablaufdiagramm für das erfindungsgemäße Verfahren.

Figur 1 zeigt ein typisches Mikroprozessorsystem, wie es auch in Steuergeräten von Kraftfahrzeugen Verwendung findet. An einem Prozessorbus PBUS ist ein Mikroprozessor CPU, ein Systemspeicher sowie eine Systemschnittstelle Interface für die Kommunikation mit externen Systemen angeschlossen. Der Systemspeicher ist logisch und funktionell in verschiedene Speicherbereiche aufgeteilt. Diese Speicherbereiche können sowohl physikalisch voneinander getrennt sein als auch durch rein logische Segmentierung

in einem physikalisch einheitlichen Speicher gebildet werden. In dem Boot-Sektor des Mikroprozessorsystems ist im Wesentlichen das Betriebssystem für den Mikroprozessor selbst abgelegt. Als Anwendungsprogramm ist in dem Boot-Sektor auch ein sogenannter Flash Boot Loader abgelegt. Mit diesem Flash Boot Loader werden bei Bedarf neue Anwendungsprogramme unter Systemschnittstelle Interface heruntergeladen und in den Flashspeicher des Mikroprozessorsystems abgelegt. Weiterhin ist im Boot-Sektor die Hash-Funktion, nämlich der sogenannte RIPEMD-160-Algorithmus, abgespeichert. Im Flashspeicher Flash des Mikroprozessorsystems sind typischerweise die Anwendungsprogramme, mit denen das Steuergerät ECU arbeitet, abgelegt. Der Flashspeicher ist ein elektrisch löschbarer und programmierbarer, nicht flüchtiger Speicher. Derartige Speicher sind als EEPROM bekannt. Für die Anwendung des erfindungsgemäßen Verfahrens enthält das Mikroprozessorsystem einen Pufferspeicher Puffer. Dieser Pufferspeicher kann als separater Speicher, z. B. als sogenannter Cash-Speicher, ausgebildet sein oder kann als reservierter Speicherbereich innerhalb des Schreiblesespeichers RAM des Mikroprozessorsystems ausgebildet sein. In dem Schreiblesespeicher RAM werden von den Anwendungsprogrammen die notwendigen Daten, Zwischenergebnisse und Ergebnisse eingelesen, abgelegt, zwischengespeichert und ausgegeben. Für die Zwecke der Authentizitätsprüfungen ist in einem besonders geschützten Lesespeicher entweder ein Schlüssel in Form eines Dechiffriercodes oder in Form eines geheimen Kennzeichnungscodes hinterlegt. Ein Dechiffriercode wird für Verschlüsselungsverfahren benötigt, während ein Kennzeichnungscode für vereinfachte Authentifizierungsverfahren, wie z. B. die Message Authentication Codes, benötigt wird. Mit einem derartig aufgebauten Mikroprozessorsystem können Anwendungsprogramme als soge-

nannte Flashware mit einem Downloadprozess, wie er beispielsweise in der deutschen Patentschrift DE 195 06 957 C2 beschrieben ist, heruntergeladen werden und in dem Flashspeicher abgelegt werden. Auch ist es mit einem Mikroprozessorsystem gemäß dem Aufbau nach Figur 1 möglich, für die herunterzuladende Flashware standardisierte Authentifizierungsverfahren durchzuführen. Als Authentifizierungsverfahren im Sinne dieser Erfindung werden zum einen etablierte Signaturverfahren, wie z. B. die Public-Key-Verschlüsselung, bezeichnet und zum anderen die sogenannten Message Authentication Codes ins Auge gefasst. Ein Beispiel eines Signaturverfahrens für Flashware, basierend auf einem Public-Key-Verfahren, ist ausführlich in der deutschen Patentanmeldung DE 100 08 974 A1 offenbart.

Bei den Public-Key-Verschlüsselungsverfahren hat sich das sogenannte RSA-Verschlüsselungsverfahren, benannt nach den Erfindern Rivest, Shamir und Adleman, als Standard durchgesetzt. Bei diesem Verfahren wird von der zu versendenden Nachricht zunächst ein Hash-Wert mit einer an sich bekannten Hash-Funktion, z. B. der Funktion RIPEMD-160, generiert. Der Sender verschlüsselt diesen berechneten Hash-Wert mit einem privaten und geheimen Schlüssel. Der verschlüsselte Hash-Wert bildet die Signatur und wird an die zu versendende Nachricht angehängt. Der Empfänger einer Nachricht entschlüsselt mit einem öffentlichen Schlüssel die Signatur und erhält dadurch wieder den vom Sender berechneten Hash-Wert. Weiter berechnet der Empfänger der Nachricht von der unverschlüsselten Originalnachricht mit der gleichen Hash-Funktion wie der Sender den Hash-Wert der Nachricht. Stimmen der Hash-Wert aus der entschlüsselten Signatur mit dem Hash-Wert, berechnet über die unverschlüsselte Nachricht, miteinander

überein, ist die Nachricht integer und authentisch. Public-Key-Verschlüsselungsverfahren erfüllen hohe Sicherheitsanforderungen an Datenintegrität und Authentizität. In Bezug auf Steuergeräte in Kraftfahrzeugen und den Downloadprozess von Flashware für diese Steuergeräte erfüllen Public-Key-Verfahren die Bedingungen für diese höchste Sicherheitsklasse für den Downloadprozess der Flashware.

Allerdings sind Public-Key-Verschlüsselungsverfahren aufgrund der aufwendigen Verschlüsselungs- und Entschlüsselungsalgorithmen aufwendig und nicht auf jedem Mikroprozessor in einem Steuergerät eines Kraftfahrzeuges einsetzbar. Beispielsweise arbeiten die Verschlüsselungsverfahren mit Gleitkommaoperationen, die von Mikroprozessoren in einfachen Steuergeräten nicht immer unterstützt werden. Authentifizierungsverfahren geringerer Sicherheitsstufe kommen ohne Chiffrierung und Dechiffrierung aus. Ein solches Verfahren hat sich als sogenannter Message Authentication Code MAC durchgesetzt. Ein Message Authentication Code arbeitet mit einem geheimen Identifizierungscode, den alle Kommunikationsteilnehmer kennen und haben müssen. Dieser Authentifizierungscode wird an die unverschlüsselte Nachricht angehängt und von der dermaßen gekennzeichneten Nachricht wird mittels einer Hash-Funktion ein Hash-Wert berechnet. Zwischen den Kommunikationsteilnehmern wird dann die unverschlüsselte Nachricht und der berechnete Hash-Wert ausgetauscht. Ein Empfänger überprüft die übermittelte Nachricht, indem er seinen Identifizierungscode an die unverschlüsselte Nachricht anhängt und hiervon, mit der gleichen Hash-Funktion wie der Sender, den Hash-Wert berechnet. Stimmen dieser berechnete Hash-Wert mit dem vom Sender übermittelten Hash-Wert überein, so gilt die empfangene Nachricht als integer und

authentisch. Die Authentifizierungsverfahren, auf der Basis der vorbeschriebenen Message Authentication Codes, haben den Vorteil, dass lediglich ein an sich bekanntes Verfahren zur Hash-Wertberechnung eingesetzt werden muss. Weitere Chiffrier- oder Dechiffrierschritte, wie z. B. eine RSA-Verschlüsselung, werden hierbei nicht benötigt. Hash-Wertfunktionen können auch auf einfachsten Mikroprozessoren ausgeführt werden. Die Anwendung von Message Authentication Codes ist z. B. durch die Patentschrift US 6,064,297 belegt. Allerdings wurden Message Authentication Codes bisher lediglich bei Internetanwendungen oder, wie im Fall der US-Patentschrift, in Computernetzwerken bekannt.

Figur 2 nimmt Bezug auf die physikalische Datenverteilung in einem logischen oder physikalischen Speicherbereich bzw. Speicherblock. In einem Speicherblock sind in der Regel nicht alle Speicherplätze mit Daten belegt. In der Regel befinden sich die Nutzdaten in einem Speicher in verschiedenen Segmenten, in denen der Speicherbereich beschrieben wurde. Zwischen den einzelnen Segmenten Segment 1, Segment 2 bis Segment N, wie in Figur 2 dargestellt, werden die nicht mit Nutzdaten beschriebenen Speicherbereiche mit sogenanntem illegal opcode oder illegal data aufgefüllt. Der illegal opcode bedeutet beispielsweise ein Anfüllen der nicht mit Nutzdaten beschriebenen Speicherbereiche mit logischen Nullen. Zur Überprüfung von logischen Speicherblöcken und zur Überprüfung von Kopiervorgängen auf Übertragungsfehler wurden in der Informationstechnologie die zyklischen Blocksicherungsverfahren entwickelt. In der englischen Bezeichnung heißen diese zyklischen Blocksicherungsverfahren Cyclic Redundancy Check, kurz CRC. Hierbei handelt es sich um eine Methode zur Überprüfung von Übertragungsfehlern mittels einer

Checksumme. Ein einfaches Beispiel einer Checksumme ist das Paritätsbit, das zu jedem 8 Byte, 16 Byte, 32 Byte, 64 Byte-langen Informationspaket als Checksumme berechnet wird und angehängt wird. Das Paritätsbit gibt hierbei Auskunft darüber, ob die Anzahl der logischen Einsen in dem Informationspaket gerade oder ungerade ist. Ein Kopiervorgang gilt dann als fehlerfrei, wenn sich die Checksumme Parität beim Kopiervorgang nicht geändert hat. Diese zyklischen Blocksicherungsverfahren werden sowohl als Checksumme über den gesamten logischen Speicherblock, d. h. Nutzdaten in den Segmenten plus aufgefüllte Lücken, berechnet als auch als Checksumme über die Nutzinformation in den Segmenten alleine. Die Checksumme über den gesamten logischen Block wird hier mit CRC_total, während die Checksumme über die Nutzdaten in den Segmenten hier mit CRC_written bezeichnet wird. Diese zyklischen Blocksicherungsverfahren zur Überprüfung des Kopiervorgangs an sich, werden auch beim Downloadprozess von Flashware in die Flashspeicher eines Steuergerätes in einem Kraftfahrzeug angewandt. Zyklische Blocksicherungsverfahren benötigen ähnlich wie eine Hash-Funktion Zugriff auf die Nutzdaten, deren Kopiervorgang bzw. deren Hash-Wert berechnet werden soll. Jedoch wurden bisher die zyklischen Blocksicherungsverfahren völlig getrennt von den mittels eines Hash-Wertverfahrens arbeitenden Authentifizierungsverfahrens durchgeführt. Das heißt, es wurden erst die Blocksicherungsverfahren durchgeführt und abgeschlossen, bevor man einen Hash-Wert für ein Authentifizierungsverfahren berechnet hat. Dadurch waren in Vergangenheit jeweils Lesezugriffe auf den Flashspeicher für die Blocksicherungsverfahren einerseits als auch im nachfolgenden Identifizierungsverfahren für die Hash-Wertberechnung andererseits notwendig.

An diesem Punkt setzt die Erfindung an.

Figur 3 zeigt ein Beispiel für einen optimierten Downloadprozess von Flashware, bei dem neben zyklischen Blocksicherungsverfahren auch ein Authentifizierungsverfahren, basierend auf einer Hash-Wertberechnung durchgeführt wird. Die in den Flashspeicher heruntergeladene Flashware wird zunächst aus dem Flashspeicher ausgelesen (read flash) und in den Pufferspeicher (refill buffer) zwischengespeichert. Im nächsten Schritt wird mit einem zyklischen Blocksicherungsverfahren über die gesamten, im Pufferspeicher zwischengespeicherten und aus dem Flashspeicher kopierten Daten eine Checksumme über den gesamten Flashspeicher berechnet. Mit dieser Checksumme CRC_total kann später die Integrität des Flashspeichers geprüft werden. In einem nächsten Abfrageschritt (data within segment?) wird abgefragt, ob der ausgelesene Flashspeicher Nutzdaten enthielt. Sind keine Nutzdaten vorhanden, wird nicht sofort ein Fehler ausgegeben, sondern erst beim Vergleich der berechneten Checksummen CRC_written mit der beim Downloadprozess übermittelten Checksumme CRC_transmitted. Die Checksumme CRC_total wird gespeichert und steht damit bei einem späteren Selbstcheck zur Verfügung.

Enthielt der ausgelesene Flashspeicher Nutzdaten, wird für diese Nutzdaten ein separates Blocksicherungsverfahren durchgeführt. Dieses Blocksicherungsverfahren für die Nutzdaten wird lediglich über diejenigen Speicherbereiche durchgeführt, in denen die Nutzdaten abgelegt sind. Die berechnete Checksumme CRC_written wird später mit der beim Downloadprozess übertragenen Checksumme für die Nutzdaten der Originalsoftware CRC_transmitted verglichen. Für einen ordnungsgemäßen Kopiervorgang während des

Downloadprozesses müssen beide Checksummen übereinstimmen. Stimmen die Checksummen CRC_written und CRC_transmitted nicht überein, wird wiederum eine Fehlermeldung „Error in CRC Verification" ausgegeben. Sofern die Flashware keiner besonderen Sicherheitsklasse unterliegt, werden an der zwischengespeicherten Flashware keine weiteren Prüfungen mehr vorgenommen. Unterliegt die Flashware besonderen Sicherheitsklassen, so werden unmittelbar anschließend an die Berechnung des CRC_written, die für die Authentifizierung der Flashware notwendigen Hash-Wertberechnungen durchgeführt. Da sich die Flashware zu diesem Zeitpunkt noch im Pufferspeicher, der im Vergleich zum Flashspeicher deutlich kürzere Zugriffszeiten hat, befindet, können die Hash-Wertberechnungen über die Daten im Pufferspeicher durchgeführt werden, was zu einem deutlich zeiteffizienteren Ablauf des Verfahrens führt. Die Hash-Wertberechnungen bzw. die Durchführung der Authentifizierungsverfahren müssen natürlich entsprechend der jeweiligen Sicherheitsklasse der Flashware durchgeführt werden. Von besonderem Interesse hierbei sind, wie im Zusammenhang mit Figur 1 bereits ausgeführt, Public-Key-Verschlüsselungsverfahren, in Form eines sogenannten RSA-Verfahrens, für Flashware mit einer hohen Sicherheitsklasse oder die angeführten Message Authentication Codes für Flashware mit einer geringeren Sicherheitsstufe.

Ist die Flashware mit einem Message Authentication Code gesichert, wird die unverschlüsselte Flashware mit dem geheimen Identifizierungscode konkateniert und über diese Kombination ein Hash-Wert HMAC berechnet. Dieser berechnete Hash-Wert HMAC wird mit dem, beim Downloadprozess übermittelten Hash-Wert HMAC_transmitted verglichen. Stimmen beide Werte überein, ist die Authentifizierung er-

folgreich (Verification ok), stimmen die beiden Werte nicht überein, wird eine Fehlermeldung ausgegeben „Error in HMAC-Verification".

Unterliegt die Flashware einer höheren Sicherheitsstufe, z. B. einer Authentifizierung durch das im Zusammenhang mit Figur 1 diskutierte RSA-Verfahren, so wird mit den im Puffer zwischengespeicherten Daten das Authentifizierungsverfahren gemäß diesem RSA-Verfahren durchgeführt. In diesem Fall wird der codiert übertragene Hash-Wert der Originalsoftware mit dem öffentlichen Schlüssel des RSA-Verfahrens dechiffriert, so dass man den Hash-Wert der Originalsoftware Hash_transmitted erhält. Sodann wird für die im Pufferspeicher befindliche Flashware ein weiterer Hash-Wert Hash (CCC) berechnet und mit dem dechiffrierten Hash-Wert der Originalsoftware Hash_transmitted verglichen. Stimmen beide Hash-Werte überein, ist die Authentifizierung erfolgreich (Verification ok). Stimmen beide Hash-Werte nicht überein, wird eine Fehlermeldung ausgegeben „Error in Hash Verification". Gelingt eine Dechiffrierung des codiert übertragenen Hash-Wertes nicht, so endet das Authentifizierungsverfahren vorzeitig und es wird eine Fehlermeldung „Error in Signature Verification" ausgegeben.

Zusammenfassend kann festgehalten werden, dass durch die Zwischenspeicherung der heruntergeladenen Flashware in einem Pufferspeicher mit schnellen Zugriffszeiten die für den Downloadprozess notwendigen Prüfverfahren zeiteffizienter durchgeführt werden können. Sowohl die zyklischen Blocksicherungsverfahren als auch die je nach Sicherheitsklasse anzuwendenden Authentifizierungsverfahren werden in dem erfindungsgemäßen Verfahren mit den im Pufferspeicher zwischengespeicherten Daten durchgeführt. Ein

mehrfacher Zugriff auf den Flashspeicher für die Durchführung der Blocksicherungsverfahren einerseits und für die Durchführung der Authentifizierungsverfahren andererseits wird erfolgreich vermieden. Dadurch ergeben sich letztlich kürzere Flashzeiten und damit eine Einsparung von Produktionszeit. Der Downloadprozess für Flashware muss nämlich bei einem Download in ein Steuergerät eines Kraftfahrzeuges zum ersten Mal während der Produktion des Kraftfahrzeuges durchgeführt werden. Die Kraftfahrzeuge können schließlich nicht mit Steuergeräten ohne Software ausgeliefert werden.

Patentansprüche

1. Verfahren zur Überprüfung der Datenintegrität von Flashware in elektronischen Steuergeräten mit mindestens einem Mikroprozessor (CPU), mindestens einem Flashspeicher (Flash), mindestens einem Boot-Sektor, mindestens einem Pufferspeicher und mindestens einer Schnittstelle (Interface) für das Herunterladen der Flashware,
d a d u r c h g e k e n n z e i c h n e t ,
dass zur Überprüfung der Datenintegrität die Flashware in einen Pufferspeicher geladen wird und das für die Flashware im Pufferspeicher mindestens zwei Prüfsummen berechnet werden, nämlich ein zyklisches Blocksicherungsverfahren zur Überprüfung auf Übertragungsfehler und eine Hash-Wertberechnung zur Überprüfung der Flashware auf Authentizität.

2. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t ,
dass für die Flashware im Pufferspeicher ein zyklisches Blocksicherungsverfahren (CRC) sowie eine Authentifizierung durch einen Message Authentication Code und eine Hash-Wertberechnung durchgeführt werden.

3. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t ,
dass für die Software im Pufferspeicher ein zykli-

sches Blocksicherungsverfahren, eine Signaturprüfung und eine Hash-Wertberechnung durchgeführt werden.

4. Verfahren nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t ,
dass die Signaturprüfung mit einem Public-Key-Verfahren erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 5,
d a d u r c h g e k e n n z e i c h n e t ,
dass nach dem Blocksicherungsverfahren eine Abfrage der Sicherheitsklasse für die zu überprüfende Software erfolgt.

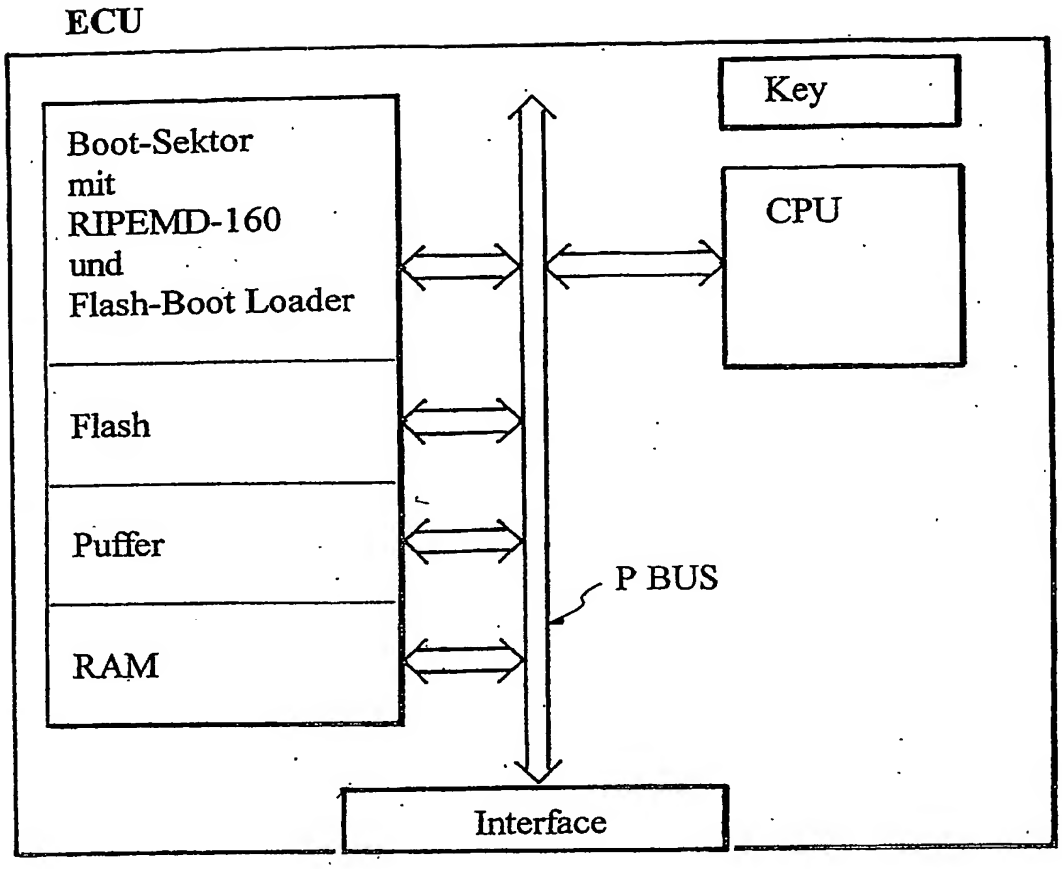

ECU
Key
Boot-Sektor
mit
RIPEMD-160
und
Flash-Boot Loader
CPU
Flash
Puffer
RAM
P BUS
Interface

FIG. 1

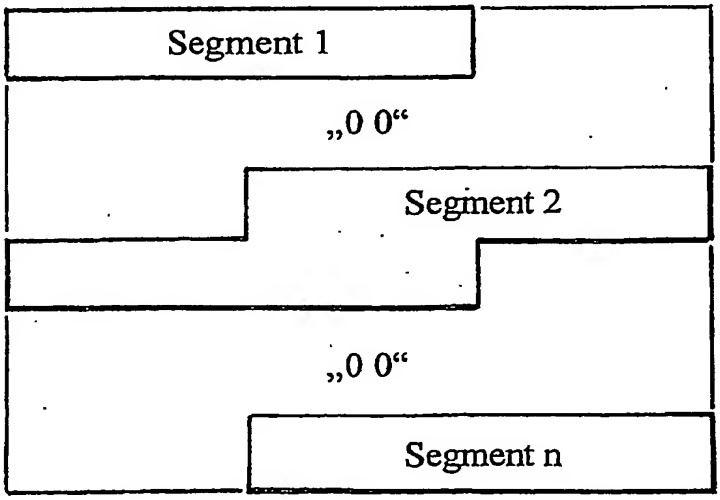

Segment 1
„0 0“
Segment 2
„0 0“
Segment n

FIG. 2

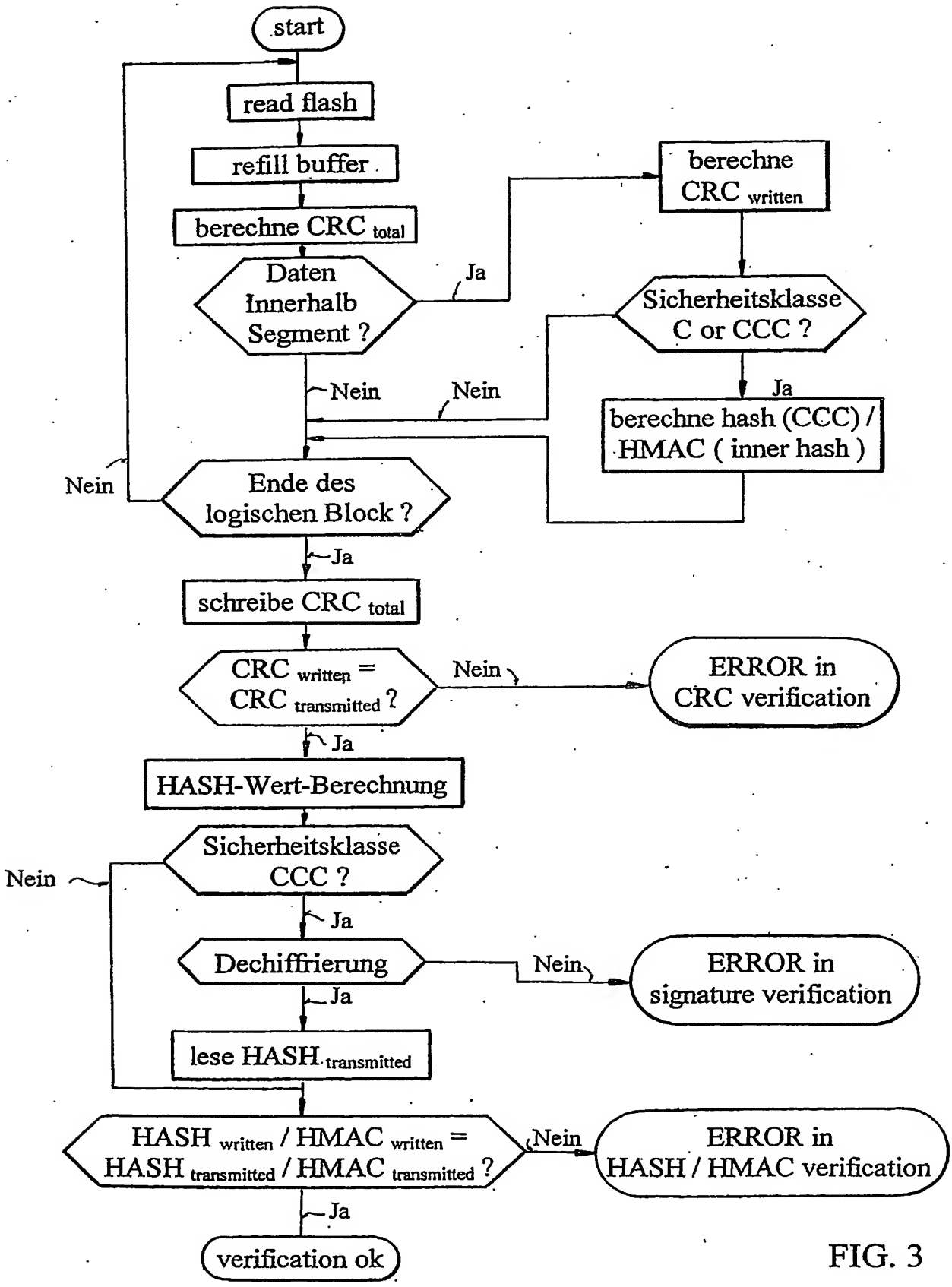

start
read flash
refill buffer
berechne CRC total
Daten Innerhalb Segment ?
Ja
berechne CRC written
Sicherheitsklasse C or CCC ?
Nein
Nein
Ja
berechne hash (CCC) / HMAC (inner hash)
Nein
Ende des logischen Block ?
Ja
schreibe CRC total
CRC written = CRC transmitted ?
Nein
ERROR in CRC verification
Ja
HASH-Wert-Berechnung
Sicherheitsklasse CCC ?
Nein
Ja
Dechiffrierung
Nein
ERROR in signature verification
Ja
lese HASH transmitted
HASH written / HMAC written = HASH transmitted / HMAC transmitted ?
Nein
ERROR in HASH / HMAC verification
Ja
verification ok

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/001807

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 195 06 957 A (SIEMENS AG) 29 August 1996 (1996-08-29) cited in the application column 2, line 53 - line 62 column 3, line 58 - column 4, line 67	1-5
Y	US 2001/007131 A1 (GALASSO LEONARD J ET AL) 5 July 2001 (2001-07-05) figure 7 paragraph '0022! paragraph '0028! - paragraph '0029! figure 4	1-5
A	US 2003/065935 A1 (NEUFELD E DAVID) 3 April 2003 (2003-04-03) paragraph '0020! paragraph '0023!	1-5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 2004	26/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fleckinger, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/001807

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 100 08 974 A (BAYERISCHE MOTOREN WERKE AG) 6 September 2001 (2001-09-06) cited in the application the whole document	1-5
A	US 5 802 592 A (SORKIN GREGORY BRET ET AL) 1 September 1998 (1998-09-01) column 1, line 37 - line 46 column 5, line 29 - line 37	1-5
A	BELLARE M: "MESSAGE AUTHENTICATION USING HASH FUNCTIONS - THE HMAC CONSTRUCTION" 1996, CRYPTOBYTES MAGAZINE, XX, XX, PAGE(S) 1-5 , XP002184520 page 1 - page 2	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/001807

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19506957 A	29-08-1996	DE 19506957 A1	29-08-1996
US 2001007131 A1	05-07-2001	NONE	
US 2003065935 A1	03-04-2003	NONE	
DE 10008974 A	06-09-2001	DE 10008974 A1	06-09-2001
		EP 1128242 A2	29-08-2001
		JP 2001255952 A	21-09-2001
		US 2002120856 A1	29-08-2002
US 5802592 A	01-09-1998	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/001807

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DE 195 06 957 A (SIEMENS AG) 29. August 1996 (1996-08-29) in der Anmeldung erwähnt Spalte 2, Zeile 53 - Zeile 62 Spalte 3, Zeile 58 - Spalte 4, Zeile 67	1-5
Y	US 2001/007131 A1 (GALASSO LEONARD J ET AL) 5. Juli 2001 (2001-07-05) Abbildung 7 Absatz '0022! Absatz '0028! - Absatz '0029! Abbildung 4	1-5
A	US 2003/065935 A1 (NEUFELD E DAVID) 3. April 2003 (2003-04-03) Absatz '0020! Absatz '0023!	1-5

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. Juli 2004	26/07/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fleckinger, C

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 100 08 974 A (BAYERISCHE MOTOREN WERKE AG) 6. September 2001 (2001-09-06) in der Anmeldung erwähnt das ganze Dokument	1-5
A	US 5 802 592 A (SORKIN GREGORY BRET ET AL) 1. September 1998 (1998-09-01) Spalte 1, Zeile 37 - Zeile 46 Spalte 5, Zeile 29 - Zeile 37	1-5
A	BELLARE M: "MESSAGE AUTHENTICATION USING HASH FUNCTIONS - THE HMAC CONSTRUCTION" 1996, CRYPTOBYTES MAGAZINE, XX, XX, PAGE(S) 1-5 , XP002184520 Seite 1 - Seite 2	2

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2004/001807

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19506957 A	29-08-1996	DE 19506957 A1	29-08-1996
US 2001007131 A1	05-07-2001	KEINE	
US 2003065935 A1	03-04-2003	KEINE	
DE 10008974 A	06-09-2001	DE 10008974 A1	06-09-2001
		EP 1128242 A2	29-08-2001
		JP 2001255952 A	21-09-2001
		US 2002120856 A1	29-08-2002
US 5802592 A	01-09-1998	KEINE	